LE CHIFFREMENT SUR LES LIENS RADIO, UNE NOUVELLE PERSPECTIVE DE PERFORMANCE ET DE SÉCURITÉ

A. Biri A. Ahmad H. Afifi

Télécom SudParis

9, rue Charles Fourier, 91011 Evry Cedex, France

RÉSUMÉ

Dans cet article nous décrivons une méthode qui change l'approche habituelle de sécurité de liens de données sans fil de la famille IEEE 802.xx (ceci inclut les réseaux locaux Wifi, métropolitains Wimax et personnels Bluetooth) basée sur la couche de liaison de données (MAC). Nous proposons deux mécanismes implantés dans la couche physique. Le premier permet une authentification basée sur la théorie de l'information et la seconde permet un chiffrement en couche physique. Ces deux méthodes apportent une grande amélioration de la sécurité et des performances. Bien que les principes restent valables pour toute technologie sans fil, nous montrons comment ils peuvent être implantés dans des prototypes de couches physiques développés dans le cadre du projet Europeen MAGNET pour un usage médical.

DESCRIPTION DU SYSTÈME

Le reste de l'article est rédigé en anglais, nous donnons dans cette section les principales caractéristiques du système et les arguments qui poussent vers une sécurité dans la couche physique.

ARGUMENTS POUR UNE COUCHE PHYSIQUE SÉCURISÉE

Dans cette section, nous argumentons en faveur du choix d'implanter la sécurité dans la couche physique.

La sécurité sur le lien radio est un choix qui reste valable même en présence de sécurité plus globale de bout en bout telles que des solutions IPSEC et TLS. Celles-ci éliminent un grand nombre d'attaques mais pas la totalité. Des attaques de type ' usurpation d'adresse MAC ' et violation de l'anonymat qui seraient fatales, restent faciles à mettre en œuvre en présence d'IPSEC ou de TLS.

La sécurité dans la couche physique a des objectifs similaires à celle de la couche MAC, mais elle offre plusieurs avantages :

- Chiffrement plus robuste contre des attaques de force brute. Il est plus difficile d'enregistrer du trafic et de tenter de le décoder dans les couches inférieures car cela nécessite du matériel difficile à pourvoir (contrairement à des sniffers classiques de couches hautes).
- Les adresses MAC sont cachées par le chiffrement et donc cela offre plus de protection et surtout l'anonymat complet.
- Avec l'authentification basée sur la théorie de l'information, on n'a pas besoin de fournir ou d'échanger d'information liée à des clés ou des secrets partagés, cela reste très facile à mettre en œuvre et offre l'avantage de facilité d'usage.

La contrepartie est que la couche physique aura une tache additionnelle de chiffrement. Cela implique plus d'intégration de logique mais à notre avis ne constitue pas vraiment de verrou en terme de mise en œuvre.

Dans la première partie, nous utilisons l'information relative au canal radio et qui varie en fonction de la position de l'équipement par rapport au point d'accès pour fournir un secret partagé unique. Il garantit ainsi l'absence d'un homme au milieu qui pourrait compromettre la dérivation de clés.

Dans le second système, nous combinons le codage canal à la sécurité et nous effectuons un chiffrement après ce codage. L'information se trouve ainsi plus sécurisée et les entêtes MAC sont en grande partie cachées. On a choisit le mode de chiffrement OFB qui permet d'éviter la propagation d'erreurs lors de la transmission sans fil.

I. INTRODUCTION

The Medical Body Area Network (MBAN) paradigm refers to a collection of tiny sensor nodes with wireless communications and limited computation capabilities dedicated for health applications. The sensors in MBAN are attached to or incorporated into a patient's body. A MBAN is in fact an emerging application for Wireless Sensors Networks (WSN). It allows a real-world achievement of concepts like ubiquitous computing. Among projects dedicated to the use of wireless sensors for medical applications, one can evoke "CodeBlue" from Harvard University. They developed wireless vital sign sensors and a scalable software infrastructure for wireless medical devices. As few research efforts addressed this issue, security in MBAN is therefore still a challenging domain.

The wireless sensors of MBAN measure collect and send patients' vital sign data to an entity, called *Personal Server* (PS), which can be hosted in the patient's Personal Digital Assistant (PDA). Data in MBANs, usually vital signs, are critical. That's why their confidentiality and integrity must be ensured. Another concern is to ensure that the sensors communicating with the personal server are really those attached to the body of the right person. So we need to protect data with means of key distribution. We do not rely on pre-distributed factory secrets in our scheme since we want to use sensors from different manufacturers and keep the network as flexible as possible. This means that the keys have to be derived completely from scratch. Another event that might trigger key refreshment is when the user gives access to some

sensors of his MBAN (for instance to his physician in hospital environment).

Our problem is to establish and maintain secure links within the MBAN as well as between each node in the MBAN and the PS. This procedure must be achieved with respect to the restricted computational capabilities and energy capabilities of MBAN. In this paper, we propose a novel key management framework for MBAN describe the design of the scheme, formal validation and evaluation of the protocol used to derive pairwise keys between two entities. Our scheme complies with the limited computational capabilities of MBANs while minimizing the user involvement.

The remainder of the paper is organized as follows: section 2 presents related work on the secure communication from an information theoretic perspective and MBANs security. The next section describes the key management scheme design and operation modes, followed by the formal validation and evaluation of the protocol used to derive pairwise keys between two entities. Finally, we conclude.

II. RELATED WORK

Information-theoretic security is one of the two main notions of security in modern cryptography. Information-theoretically secure systems are impossible to break even for adversaries with unlimited computational power in contrast to computationally secure cryptosystems, which provide security against computationally bounded adversaries [1]. The laws of physics place a bound, in certain contexts, on the amount of information an adversary can obtain. Li and al [2] propose to establish new forms of authentication and confidentiality that operate at the physical layer based on the fact that the radio channel decorrelates rapidly in space, time and frequency. The fact that pairwise radio propagation laws between two entities are unique and decorrelates quickly with distance is used for the establishment of shared secrets. They validate the feasibility of using physical layer techniques for securing wireless systems by presenting results from experiments involving the USRP/GNURadio software defined radio platform.

The related work concerning MBAN security is as follows:

Cherukuri et al. [3] proposed a biometric-based approach for securing communication in a wireless network of biosensors implanted in the human body. They used a commitment scheme which tolerates errors in the encryption key within a specified range [4]. Using such encryption scheme is useful in scenarios where biometric traits are used. If a biosensor has to send data to another one, it generates a random key named $K_{session}$ and encrypts the data with this key. Then, $K_{session}$ is committed by another key, named K_{commit}, which is computed from the biometric measured from the body. Thereafter, the encrypted data and is sent along with the commitment of the session key. Upon the reception of the message, a biosensor decommits the session key using its K_{commit} and then retrieves data. They suggest using pre-deployed keys to communicate with the controller node that is the PS.

Bao et al. [5] describe security architecture for body sensors networks. This architecture consists of a master node which is a wearable biomedical sensor, and slave nodes which are biosensor implanted in the human body. Upon the reception of a synchronization indication from the master node, the slaves capture auto-shared secret (ASS) via a so-called bio-channel. An ASS is a set of biometric values extracted from physiological data, simultaneously collected by nodes during a certain period of time. Then, the master node uses the ASS in order to protect the transmission of a key named K_{init} to the slave nodes. K_{init} will then be used to protect the transmission of session keys. Bao et al. [6] describe a feasibility study of using intrinsic characteristic of a human body to securing the distribution of a cipher key to BASN sensors. Sensors can either be wearable or implanted in the body. They use the inter-pulse interval as a biometric characteristic for the generation of ASS. The method was tested on 99 subjects with 838 segments of simultaneous recordings of electrocardiogram and other vital measurements. The system achieved a minimum half total error rate of 2.58%. In fact, they show good similarity between identities (physiological data captured by one node) in the same MBAN. They also proved that there is a big difference between two identities of the two sensor nodes from different MBANs. The results of statistical analysis suggest that such measurements are suitable biometric feature for the entity authentication of MBANs.

Malasri and al [7] proposed a public key based architecture and security protocol to achieve security requirements for a medical sensor network. The cornerstone of this proposition is the use of fingerprints of the user. In fact, sensor nodes generate a random number and a master key from the patient's fingerprint. Then, they exchange messages with the base station (equivalent to the PS) using these values in order to get a shared secret with the base station. They evaluate their protocol based on an implementation of Elliptic Curve Cryptography (ECC) for the Moteiv's Tmote Sky platform. The security offered by the proposed solution requires patient's fingerprint as reliable identifier. This solution has security vulnerabilities since it is obvious nowadays that fingerprints can be imitated quite easily.

Seo and al [8] propose a cluster-based Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) [9] to provide efficiency and security during the pairwise key setup and broadcast authentication phases, respectively. ECC offers asymmetric cryptography with considerably lower computational burden and smaller key sizes than traditional asymmetric cryptosystems and thus, is fully convenient to a protocol involving a sensor network. They have implemented their protocol on 8-bit, 7.3828-MHz MICAz mote. Their experimental results indicate the feasibility of their protocol for wireless sensor nodes. Note that the sensors used in this implementation are also used for the implementation of wearable sensor nodes.

Several solutions have been proposed to derive keys in the case of a combination of low power and full function devices. Merkle's puzzle [10] is the most credible solutions in this field. Merkle's puzzle is one of the first protocols for key

exchange without assuming any prior secrets. Merkle's puzzle is used between a constrained device denoted here by A and a more powerful device denoted here by B. So MP seems to be a good candidate to generate keys between sensor node in the MBAN and the personal server which is hosted for example by the PDA as the SP. A puzzle consists on a random puzzle id, a random cryptographic key K and some redundant information. The puzzle is encrypted by a key k which is smaller than K. The device B sends N puzzles to the device A. The device A chooses randomly a puzzle, recovers the plain text of the puzzle by a brute force attack which is feasible since k is small and tells B the id of the puzzle he has chosen. The device B uses the id received from the device A to know the key chosen by A. The attacker here can be more powerful that the constrained sensor node and so he can perform the same computations as the constrained device in less time so we will not consider this protocol in our solution.

III. PROPOSED SOLUTION

The use case of a MBAN is illustrated by figure 1: several bio-sensors collect data on a patient's body. The data is sent to a PDA, acting as the PS. The data is thereafter conveyed via a wireless access (WLAN for instance) to a remote hospital. Our goal in the remainder of the section is to provide robust and fresh key material for the MBAN to the PS communication.

A. Overview

In our solution, we propose to use asymmetric cryptography to generate a pairwise key between two nodes within the MBAN or between MBAN's node and the PS. Thus, we respect the computational capabilities of nodes since we use asymmetric cryptography only to derive pairwise key. We use a personal certificate authority, located in the Personal Server, which distributes certificates to MBAN nodes. In fact, using digital certificates is an established method to generate trusted identities in network communications. As we have to optimize the battery consumption, we will organise the MBAN into clusters. A cluster is a group of co-located sensors which delegate one of them, for short periods of time, in order to perform direct communication with the personal server.

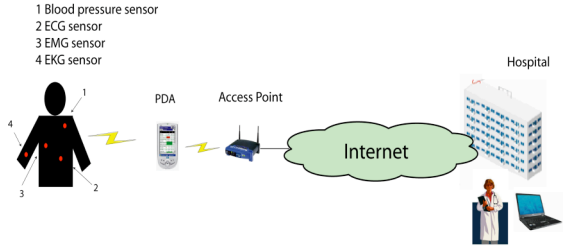

Figure 1: A general MBAN use case

We have to distinguish two phases: deployment phase and usage phase. The deployment phase represents the phase where MBAN's sensors are attached to the body. The usage phase begins when deployment phase ends and corresponds to the MBAN's operational phase. In the following sections, we will describe this two phases in detail.

S_I	a sensor node of the MBAN
$Pub(S_I)$	public key of sensor node S_I
$Pri(S_I)$	private key of sensor node S_I
{.}_K	encrypted using key K
ID_{SI}	identifier of S_I
H(.)	a one-way secure hash function
S	secret
N_{SI}	a random number generated by S_I
Pub_C_(PS)	public key of the certification authority hosted by PS
$Cert_{SI}$	the certificate of sensor node S_I

B. Deployment phase

The deployment phase represents the phase where the sensors are attached to the body of one user. The user secures the deployment phase by starting the personal server. It consists in four steps.

In step 1, upon the reception of a synchronization indication from the PS, the MBAN's node get simultaneously physiological data during a certain period of time. Each node will then extract biometric values from this data in order to obtain the "bio" key K_{bio}. Then, PS and S obtain a shared key using information-theoretic security. In step 2, each node of the MBAN gets a certificate from the PS. In step 3, we propose to use the secure cluster formation process described in [11] in order to organize the MBAN into cluster. In fact, they use physiological values in order to secure the process of the formation of clusters. In the last step, sensor nodes derive pairwise keys between them and with the PS. The security offered by this phase requires little user involvement.

1) First Step

In step 1, all the sensors of MBAN receive a synchronization frame from the PS in order to capture physiological data and thus to obtain the K_{bio}. The synchronisation frame contains the PS's identifier and synchronisation information (physiological data capture's periodicity for example). Each biomedical sensor sends a frame to the PS containing its identity and computational resources. The PS chooses the most powerful sensor S. As the PS cannot assume that the sensor S is talking to, belongs to the legitimate patient, the patient has to be on a specific location such as the attacker is not able to be on the same location at the same time. Thus, the PS verify the sensor S's position by asking positioning system like proposed in [12]. In order to obtain a shared key from the physical layer between PS and S, we choose the same physical layer model and method proposed by Li and al [2] and consisting in channel state masking. In fact, it's in our point of view the simplest proposed method in order to share a secret between Alice and Bob from an Information-theoretic security perspective. To obtain $K_{1, Alice}$ and Bob estimate first their channel state information and they convert the obtained

values to a binary representation using quantization process. They then use using them as the key sequence in a one-time pad to mask the key being distributed.

2) Second step

PS delivers certificates which are used to bind the identities of MBAN nodes to their long term ECDH public key. This ensures that once the certificates are issued by the PS and while they are neither revoked nor expired, the identities and their long term ECDH public keys are trustable by all MBAN nodes. Certificates will be used for mutual authentication between two entities who wants to derive pairwise key.

The messages exchanged between each S_I of the MBAN and the PS are as follows:

PS--> S: {Pub_C_(PS)|ECDH_CP}_K_1
S --> S_I: {Pub_C_(PS)|ECDH_CP}_K_{bio}
// here S_I generates its public and private key
S_I --> S :{Pub (S_I) | ID S_I }_ K_{bio}
S --> PS :{Pub (SI) | ID SI }_ K_1
PS-->S: {$Cert_{SI}$ }_K_1
S-->S_I: {$Cert_{SI}$ }_K_{bio}

All data encrypted by K_{bio} must be error-correcting code with the ability of correcting k-bit errors because K_{bio} obtained by different nodes may have a difference of up to k bits [5].

The PS sends the concatenation of its signature public key and the ECDH common parameters encrypted by K_1 to S which will send them to all MBAN's nodes encrypted by K_{bio}. The ECDH common parameters will be used for future ECDH operations. Each S_I decrypts it using K_{bio} and store the PS's signature public key. Then, Each S_I computes his public and private key and sends its identifier and public key encrypted by K_{bio} to S which will forward it to PS encrypted by K_1. The PS decrypts each message from each S_I using K_{bio} and then issue a certificate for S_I. Upon the reception of the message from PS, a node S_I process the verification of certificate using the PS's signature public key and store it for future use. Note that S also obtains its certificate by sending its identifier and public key to the PS.

3) Deriving pairwise key

We propose a protocol for deriving pairwise key with respect to the computational capabilities of the nodes of the MBAN.

Now each pair of nodes A and B, which could be two MBAN's nodes or a MBAN node and the PS, are able to derive a pairwise key by using these messages.

A --> B: $ID_A|Cert_A|\{N\}\_ K_{bio}$
B --> A: $ID_B|Cert_B|\{N_B|ID_B\}\_K_{ECDH}$
A --> B: $\{N_A|N_B\}\_K_{ECDH}$
B --> A: $\{N_A\}\_K_{ECDH}$

A and B then compute pairwise key K=H (N_A, N_B, N).

The following messages are exchanged over the insecure channel. In message 1, A sends its identifier, its certificate and a nonce N encrypted by K_{bio}. B verifies the certificate of A using the PS's public signature key, picks a nonce N_B and compute the K_{ECDH} [9]. He encrypts then the concatenation of its identifier and the nonce N_B with K_{ECDH} and sends the result along with his identifier and certificate. A verify the certificate of B, compute K_{ECDH} and then decrypts message 2 using K_{ECDH} and extracts N_B. Then, device A picks its nonce N_A and sends both nonce encrypted by K_{ECDH}. Finally, B decrypts the third message and sends back N_A, ciphered by K_{ECDH}. At the end of the protocol, both nodes are able to derive the long-term pairwise key as K=H(N_A, N_B,N) and to store it. Note here that the random number can be generated for sensor node from existing physiological signals [5].

C. Usage phase

The usage phase corresponds to the operational phase of the MBAN. The MBAN's owner may need operations like the addition of new sensor node or the detection and revocation of compromised nodes. The patient may also need to give access to some nodes in his MBAN for other persons, like his doctor. We have also to ensure the security within each cluster.

1) Addition of new sensor nodes to the MBAN

The MBAN's owner may need during the usage phase to add a new biomedical sensor denoted here by S_N. The user has to start the addition process in the PS. S_N sends an empty certificate_request encrypted by K_{bio} to his neighbors S_{NJ}. Then S_N choose randomly one node S_{NJ}^* between the neighbors who responds to it. Then S_N will send to S_{NJ}^* a certificate_request. S_{NJ}^* decrypt the message using its K_{bio} and then will forward the certificate request to the PS by adding the identity of its current cluster head. The PS will send a certificate for S_N to S_{NJ}^* who will relay it to S_N. The PS will then ask the cluster head of the cluster of S_{NJ}^* to add S_N to the cluster.

2) Granting access to other uses

The MBAN's owner may need to give access to some sensors of his MBAN for persons of his trust for example for his doctor in hospital environment. So our PS will give a certificate to the trusted person's device. It could be by means of pairing protocol without a priori knowledge [13]. We suggest that the pairwise key between the MBAN and the trusted person's device have to be ephemeral because of the limited storage space.

3) Key management within a cluster

Each node in the MBAN will periodically refresh K_{bio}. Each cluster head (CH) periodically sends a shared key named $K_{cluster\_i}$ encrypted by K_{bio} to each member of its cluster. The members are then able 1) to encrypt their data with the pairwise key shared with the PS then 2) with $K_{cluster\_i}$ and then 3) send the result to the cluster head.

In order to optimize the energy consumption of all the nodes in the MBAN, there is a periodic change of the CH within a cluster. The selection of the new CH is out of the scope of this paper. The current CH will send the identity of the newly elected cluster head to the PS.

4) Detection and revocation of compromised node

An adversary may add a malicious node in order to send fake data, but since this node didn't belong to any cluster, he will be detected as an unauthorized node. In fact, joining a cluster is either made in the deployment phase or with the help of the PS in the addition phase.

Besides, when an attacker steals a member of a given cluster, this will be detected by its cluster head as a corrupted node since the data it sends is not encrypted with the current $K_{cluster\_i}$. Moreover, when an adversary steals a cluster head, the node will be detected by the PS as a corrupted node as the data it sends will not comply to the form explained previously since the adversary didn't possess all the pairwise keys of the members of the cluster with the PS. In case of the detection of a corrupted node, his certificate will be revoked.

5) Encryption at the physical layer

We believe that we have to encrypt communication between biomedical sensors at the physical layer (using AES for example). In fact, it gives several advantages over classical encryption in the upper layers such as preventing some kinds of attacks or making them more difficult in term of realization, as it is much more difficult to build lower layer analysers. In order to minimise the power consumption and to avoid that each sensor first decrypts the frame in order to know if this frame is destined to him or not, we have to define a mechanism to determine the identity of the sender before the decryption process.

IV. VALIDATION AND EVALUATION

In this section, we show how we validated the proposed protocol for deriving pairwise keys. We also provide a preliminary performance evaluation in terms of computation times.

A. Automatic Validation through AVISPA

We used Automatic Validation of Internet Protocols and Application (AVISPA) tool [14], a comprehensive security protocol analyzer in order to validate our protocol. It has been used to model and validate many well known protocols, revealing already known or new flaws. AVISPA uses a High Level Protocol Specification Language (HLPSL) to describe security protocols and specifying which security goals are achieved by a given protocol. We have employed Dolev-Yao intruder model in which all communications with the intruder are synchronous [15]. In other words, the intruder is in full knowledge of all messages to and from the honest participants. The intruder has also the capability of replaying the old messages. We have used OFMC [16] tool since it provides support for specific algebraic properties, in our case the exponential operator used for ECDH key agreement. We correctly compiled HLPSL model and validated our protocol.

```
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/avispa/web-
interfacecomputation/./tempdir/workfilet19122.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.09s
visitedNodes: 33 nodes
depth: 6 plies
```

The output shows that the security goals after the validation process are reached and that the protocol is safe (that is no attack was found). These goals are mutual strong authentication between the two entities and the secrecy of N_A and N_B. Besides, OFMC was successfully run with the anti-replay option, which means that even if the intruder witnesses multiple instances of this, it will not be able to replay or forge messages and threaten the above mentioned security goals.

B. Performance evaluation

The key length used here is 163 bits which is the NIST's recommended key size. The generation of the shared secret K_{ECDH} and the verification of certificate with ECDSA are known to consume respectively 34.173 sec and 23.63 sec on the MICA II 8-bit with 7.38 Mhz CPU [17].

As for the encryption, we found 33.6 ms, 22.3 ms and 20 ms for messages 2, 3 and 4 respectively. The generation of a nonce in the sensor node takes almost 10ms.

Since generation of the shared secret K_{ECDH} and the verification of certificate with ECDSA are predominant, our next effort will be to improve the performance of these public key operations as suggested in [8].

V. CONCLUSION AND FUTURE WORK

The Medical Body Area Network is an emerging application for Wireless Sensor Networks. The need to secure communication for MBANs is obvious since sensors convey critical data. In this paper, we described a new key management scheme for Medical Body Area Networks. We proposed to cover the deployment and usage phase of MBAN. The proposed scheme requires little user involvement and meets the constrained computations capabilities of tiny sensor nodes. We validated the pairing protocol used to provide keys in order to secure communication between each node of the MBAN and the PDA. Future work will focus on its implementation.

REFERENCES

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and Steven W. McLaughlin. Information-Theoretic Security for Wireless Channels: Theory and Practice. Information Theory and Applications Workshop, San Diego, USA, February, 2007.

[2] Zang Li, Wenyuan Xu, Rob Miller and Wade Trappe, "Securing Wireless Systems via Lower Layer Enforcements," in Proceedings of the 2006 ACM workshop on Wireless security(WiSe), pg. 33-42, 2006

[3] S. Cherukuri, K.K. Venkatasubramanian and S.K.S.Gupta, ''BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body'', in Proc. IEEE Int. Conf. on Parallel Processing Workshops, Oct. 2003, pp. 432 –439

[4] A. Juels and M. Wattenberg,, ‘‘A fuzzy commitment scheme’’, in Proc. 6th ACM Conf. Computer and Communications Security, G. Tsudik, Ed., 1999, pp. 28---36.

[5] S.D. Bao, L.F. Shen, and Y.T. Zhang**, “**A Design Proposal of Security Architecture for Medical Body Sensor Networks**”,** in Proc. International Workshop on Wearable and Implantable Body Sensor Networks (BSN'06**)** pp. 84-90

[6] C.C.Y. Poon, S.D. Bao, and Y.T. Zhang, “A novel biometrics method to secure wireless body area sensor networks for telemedicine and mobile healthcare”, IEEE Communication Magazine (special issue on telemedicine), April, 2006.

[7] **K.** Malasri and L. Wang, “SNAP: an architecture for secure medical sensor networks”**,** Wireless Mesh Networks, 2006, (WiMesh 2006). pp. 160-162.

[8] S. C. Seo, Hyung-Chan Kim and R. S. Ramakrishna, “A New Security Protocol Based on Elliptic Curve Cryptosystems for Securing Wireless Sensor Networks’’, in Proc. EUC Workshops 2006, pp. 291-301.

[9] J. López, and R. Dahab, “An Overview of Elliptic Curve Cryptography’’, Technical Report IC-00-10, State University of Campinas, 2000

[10] R. Merkle, “Secure Communications over Insecure Channels”, Communications of the ACM, April 1978, pp. 294-299.

[11] K.Venkatasubramanian and S.K.S.Gupta, ‘‘Security For Pervasive Health Monitoring Sensor Applications’’, in Proc. of 4th International Conference on Intelligent Sensing and Information Processing (ICISIP), Bangalore, India, December 2006.

[12] Masashi Sugano, Tomonori Kawazoe, Yoshikazu Ohta, and Masayuki Murata, "Indoor Localization System Using RSSI Measurement of Wireless Sensor Network Based on ZigBee Standard," The IASTED International Conference on Wireless Sensor Networks (WSN 2006) , Banff (Canada), July 2006.

[13] C. Gehrmann, C. Mitchell and K. Nyberg, “Manual Authentication for Wireless Devices”, “Manual Authentication for Wireless Devices”, Cryptobytes, 7 no.1,pp. 29-37, Spring 2004.

[14] The AVISPA project homepage : http://www.avispa-project.org

[15] L. Lamport. “The temporal logic of actions”. ACM Transactions on Programming Languages and Systems, 16(3):872923, May 1994.

[16] D. Basin, S. Modersheim, and L. Viganno. “OFMC: A Symbolic Model-Checker for Security Protocols”. International Journal of Information Security, 2004.

[17] D. J. Malan, M. Welsh and M. Smith, “A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography”, In Proc. of The First IEEE International Conference on Sensor and Ad Hoc Communications and Networks (IEEE SECON), Santa Clara, California, October 2004.